WHAT IS CLAIMED IS:

1. A method of key-management in Distributed Sensor Networks, comprising the steps of:

prior to deployment of a plurality of sensor nodes of the Distributed Sensor Network, storing, in each sensor node of the Distributed Sensor Network, a respective key ring formed of randomly selected keys, a respective pair of said key rings sharing, with a predetermined probability, at least one key;

upon deployment of said plurality of the sensor nodes of the Distributed Sensor Network, discovering by at least one sensor node of said plurality of the sensor nodes for at least another sensor node sharing said at least one key with said at least one sensor node to establish a secure communication link between said one and another sensor nodes; and

using said at least one key for secure communication between said at least one and another sensor nodes over said secure communication link established therebetween.

2. The method of Claim 1, further comprising the steps of:

generating a key space,

randomly selecting a pool of keys from said key space,

assigning a specific key identifier for each key from said pool of keys, and

for each said sensor node of the distributed sensor network, randomly selecting a distinct set of the keys to form said respective key ring.

3. The method of Claim 2, further comprising the steps of:

assigning to each said sensor node a specific sensor identifier.

4. The method of Claim 2, further comprising the steps of:

loading to said at least one sensor node a specific key identifier of each key on said key ring of said at least one sensor node, and

broadcasting said key identifiers associated with said at least one sensor node to discover said at least another sensor node.

5. The method of Claim 3, wherein said Distributed Sensor Network further includes a plurality of controller nodes associated with said sensor nodes in a predetermined order, further comprising the steps of :

saving said key identifiers of the keys in said respective key ring of each said sensor node along with said sensor identifier of said each sensor node on a trusted controller node from said plurality of controller nodes.

6. The method of Claim 4, wherein said key identifiers are broadcast in a clear text.

7. The method of Claim 4, wherein said key identifiers are broadcast in a hidden pattern.

8. The method of Claim 5, further comprising the steps of:

computing a sensor-controller key shared by said each sensor node with said trusted controller, and

loading said trusted controller and said each sensor node with said sensor-controller key.

9. The method of Claim 5, further comprising the steps of :

upon compromising of at least one sensor node, revoking said at least one compromised sensor node by broadcasting from said trusted controller a revocation message containing a signed list of the key identifiers of the key ring of said compromised sensor node to be revoked.

10. The method of Claim 9, further comprising the steps of:

generating a signature key for said list and unicasting the same to each said sensor node.

11. The method of Claim 10, further comprising the steps of :

upon obtaining of said signature key by an uncompromised sensor node,

verifying said signature key of said signed list of the key identifiers of the key ring of said compromised sensor node,

locating said key identifiers in said key ring of said uncompromised sensor node, and

removing keys corresponding to the key identifiers of the compromised keys from said key ring of said uncompromised sensor node.

12. The method of Claim 9, further comprising the steps of:

reconfiguring the communication links of the sensor nodes affected by revocation of said compromised sensor node.

13. The method of Claim 1, further comprising the steps of:

upon expiration of at least one key shared by said at least one and another sensor node, removal of said expired at least one key from said key rings of said at least one and another sensor nodes, and searching for another key common for said at least one and another sensor nodes to establish a new communication link therebetween.

14. The method of Claim 2, further comprising the steps of:

generating a connectivity random graph for said Distributed Sensor Network , and

computing the number of the sensor nodes, the number of keys in said pool of keys and the size of each said key ring, sufficient to provide for a connected Distributed Sensor Network.

15. The method of Claim 1, further comprising the step of:

assigning a path-key to a selected pair of sensor nodes connected by at least two communication links.

16. A Distributed Sensor Network system, comprising:

at least two sensor nodes, each said sensor node being pre-loaded prior to deployment thereof with a respective key ring formed of randomly selected keys, said respective key rings of said at least two sensor nodes sharing, with a predetermined probability, at least one key, and

means associated with at least one of said at least two sensor nodes for searching for another of said at least two sensor nodes sharing said at least one key with said at least one sensor node to establish a secure communication link therebetween.

17. The Distributed Sensor Network system of Claim 16, further comprising:

means for generating a key space,

means for randomly selecting a pool of keys from said key space,

means for assigning a specific key identifier for each key of said pool of keys, and

means for randomly selecting at least two distinct sets of keys from said pool of keys, thus forming said respective key rings for said sensor nodes.

18. The Distributed Sensor Network system of Claim 17, wherein each said sensor node is further pre-loaded prior to deployment thereof with said key identifiers for each key of said respective key ring pre-loaded on each sensor node.

19. The Distributed Sensor Network system of Claim 17, further comprising:

at least one controller node associated with said one sensor node, said at least one controller node having said key identifiers of said key ring of said one sensor node and a specific sensor identifier of said at least one sensor node saved therein, and

means for broadcasting said key identifiers of said respective key ring.

20. The Distributed Sensor Network system of Claim 19, further comprising means for generating a revocation message and broadcasting the same for revocation of a compromised at least one of said two sensor nodes, said revocation message containing a signed list of said key identifiers of said key ring of said compromised sensor node.

21. The Distributed Sensor Network system of Claim 20, further comprising means for reconfiguring communication links of said at least another sensor node affected by revocation of said compromised sensor node.

22. The Distributed Sensor Network system of Claim 1, further comprising means for assigning a path-key to a selected pair of sensor nodes connected by at least two communication links.